The Changing Face of Education
Risk, Security and Process Around Distance Learning

The digital revolution has changed many industries, including education. Although digitized learning platforms have made education and information more easily accessible, they have also brought on a rise in cybersecurity and other process risk that must be addressed. These issues are prevalent in distance education from a security, risk and process perspective; however, there are effective methods that can be used to mitigate the risk.

Benefits of Digitization in Education
There are many benefits of digitization in learning and education. Some of the benefits include greater reach, flexibility and lower cost.

Greater Reach
Online course delivery greatly increases the reach of learning and education. Education that once was for a privileged few with online distance learning is now accessible to everyone with access to basic technology irrespective of age, gender or geography. Anyone can enroll in online courses from top universities on learning platforms such as Coursera, Udacity and Udemy. Users can apply for online degrees and even complete graduate and doctorate degrees via online distance education.

Flexibility
Another significant advantage of online distance education is flexibility. Be it working parents, full-time employees or retirees living on a different continent, education and learning can be accessed conveniently anytime via online distance education. This provides greater opportunities without having to choose between education and other priorities such as time with family or working full time.

Cost
Where an average online student pursuing distance education spends approximately US$100 to US$400 per credit hour,1 the traditional on-campus student spends multiple times that cost. The fact that most study materials including books and other reading materials are online is also an important factor when considering learning costs.

Disadvantages of Digitization in Education
Even though the benefits greatly outweigh the drawbacks, disadvantages to online distance education do exist. The main disadvantages are the same issues that affect most digitized portals: endpoint security, privacy and process issues.

Malicious Software
Online education faces threats from malware or malicious software, such as viruses, worms, ransomware, Trojan horses, keyloggers, rootkits, spyware and adware.2 In fact, the most common malicious software that affect online education are riskware and adware.3

With many students using personal laptops for

Glorin Sebastian, CISA, CISSP
Is an IT risk and security senior consultant at one of the Big Four accounting firms and has more than six years of relevant experience. He specializes in System Analysis Program Development (SAP) IT, and business and security controls.
online education and work or personal purposes, there is a high possibility of laptops being affected by malicious software, causing various issues such as affecting the operability of computers and computer networks, hardware failure, and data loss or data theft, thereby potentially negatively affecting the quality of the online learning experience.

Hacking and Denial-of-Service Attacks
A denial-of-service (DoS) attack is meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks have proliferated on online learning platforms, especially when using video conferencing applications such as Zoom. Ransomware and DoS attacks are to be expected, as schools and universities can be considered easy targets because they tend to have fewer security controls compared to enterprises. Enterprises typically have internal audit and security teams that review their IT infrastructure and suggest continuous improvements. Most educational institutions have limited resources to devote to IT security. For example, recently a US State of Nevada school district’s wages data were leaked after the school failed to pay bad actors. Another example occurred in the State of North Carolina, where a DoS attack that targeted a school district’s servers and encrypted information took down the servers and school Internet, causing school to shut down for days. In Virginia, USA, a ransomware attack occurred that obtained a Windows credentials extract from the school district servers, which included sensitive information such as student data and administrative documents. Student data on education portals are subject to the US Family Educational Rights and Privacy Act (FERPA) and other US federal privacy regulations, which govern access to educational records by public entities. FERPA also clearly forbids the disclosure of confidential student information (e.g., name, student identification number or Social Security number) in a personally identifiable manner, without the student or authorized party’s written consent. Thus, the increased risk of ransomware attacks and DoS attacks is a major threat that online distance education providers need to address.

Spoofing, Fraud and Data Theft
Spoofing, fraud and data theft also pose major issues for online education users. Spoofing, which includes fake portals disguised as a source known to the receiver, is often used by fraudsters to obtain authorization and details of students such as passwords and other sensitive information. This could lead to data theft, specifically personal and student data, which could be under the purview of privacy regulations such as FERPA and the US Children’s Online Privacy Protection Act (COPPA).

Confidentiality and Integrity Issues
Confidentiality and integrity of submitted work is also at stake when it is submitted online. It is possible that students could access other students’ data and information including submitted work, which could greatly affect the reputation of the course and the institution providing the learning opportunity. If there are not enough measures to ensure that the student course and personal data are secured, the confidentiality of the student data could be in jeopardy. Universities and other educational institutions should also consider using emerging technologies such as data analytics and blockchain, and enable trusted data sharing using a decentralized network of peers accompanied by public ledger. For example, blockchain is of genuine value in the identity and access management (IAM) space; however, there is a consensus that private information should not be stored on public blockchain networks. Rather, only individuals’ unique cryptographic identifiers should be stored and referenced. Online education must also be compliant with FERPA and other pertinent state, federal and international privacy regulations.

Conducting Online Examinations
Another important issue with online distance education is effectively conducting online examinations and assessments. Conducting examinations properly is crucial for ensuring the validity of the learning certificate. One solution for conducting online examinations is using an online proctor to ensure that students are not cheating;
however, this is challenging, given that the latest technologies such as smart watches and smart goggles make it easier for students to cheat on tests. To maintain the integrity of the exam questions, it is necessary to ensure that students do not share details of the exam with classmates. It is not always possible for a live person to proctor an exam, and often universities make use of online proctoring software. However, rigorous studies need to be conducted to ensure that these software are effective in preventing cheating.

Human Error
Forty-seven percent of business leaders say human error, such as accidental loss of a device or document, have led to data breaches within their organizations. This is a risk for online distance learning as well. Users need to be aware of the cyberthreats on an online learning platform and ensure that they follow recommended best practices such as using the university’s virtual private network (VPN) when connecting to the university network and using multifactor authentication (MFA) whenever possible.

Many privacy and security issues can be addressed using proper forms of authentication including 2FA.

Solving Security, Privacy and Process Issues
Many steps can be taken by educational institutions to solve security, privacy and process issues, including:

• Installing appropriate antivirus software—The issues relating to viruses, Trojan horses and worms can be addressed by ensuring that the school or the user has proper, updated antivirus software. Antivirus software is effective, but it should not be the only protection for a user’s computer and should be combined with other solutions that effectively protect against cyberattacks.

• Proper forms of authentication including two-factor authentication (2FA)—Many privacy and security issues can be addressed using proper forms of authentication including 2FA. Even comparatively weak 2FA through Short Message Service (SMS) messages to a phone is effective in preventing 100 percent of automated attacks, 96 percent of bulk phishing attacks and 76 percent of targeted attacks. The use of effective authentication and authorization processes can address issues relating to spoofing and ensure the confidentiality of student work and personal data.

• Remote scanning and prevention of unauthorized software installation—One way of managing cyberrisk is the remote scanning of systems and prevention of unauthorized software installation. Depending on the institution policy of students using their personal devices for learning, it may not always be possible to implement this, but enabling remote scanning, which can be done even for antivirus scans, is an effective method that educational institutions should consider while suggesting effective measures against cybersecurity threats.

• End user training—End user training is one of the most important ways to thwart a cyberattack. Making sure learners are aware of the cyber best practices relating to access and authorization and proper training for cyberawareness are tremendously helpful. This training could be videos explaining cyber best practices followed by a short quiz to ensure that students understand the topic. This type of training and education helps address the cybersecurity risk associated with online distance learning.

Conclusion
Distance education has been revolutionized by the Internet. It has removed many of the barriers of age, gender, geography and social class that previously existed in education. There are many benefits to distance learning; however, there are also drawbacks, including security, privacy and process-related issues. Having the proper controls with regard to authentication and authorization of the user, using antivirus, using remote scanning of systems, and implementing end user training can
help reduce the cyber risk related to online distance learning and ensure the integrity and confidentiality of the coursework, student achievement and personal information.

Endnotes


5 Palo Alto Networks, "What Is a Denial of Service Attack (DoS)?" https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos


